

Auditing of Information Systems (SOX)

Blake Burdett

Jacksonville University

Dr. Baker

DSIM 518

Table of Contents:

1. Abstract.....	Pg 3
2. Paper	Pg 4-6
3. References.....	.Pg 7-8
4. Appendix.....	A1-A10

Abstract

This paper examines the auditing of information systems under the law of Sarbanes Oxley (SOX). The role of auditing and the process by which an organization uses internal controls and the audit to mitigate risk associated with their information systems to generate financial reports is discussed. In addition, the costs and benefits of proper internal controls and the auditing of information systems are examined.

All over the world company's rely heavily on information systems to help run their organizations and stakeholders demand assurance that information they receive is timely and accurate. After the scandals of Enron and World Com, Sarbanes Oxley (SOX) was passed in November 2002 to help install confidence in financial reporting. While auditing has always been a significant part of most organizations, SOX 404 put stringent regulations in place to ensure that organizations report on the effectiveness of their internal controls (Klamm & Watson, 2009). Since large organizations rely on information systems to generate their financial reports, the systems must be audited to ensure that there are no material misstatements due to a failure with the systems. While auditing can be a costly endeavor, it is imperative for the sake of the organization to have proper auditing of their information systems to help ensure that risk is heavily mitigated.

The passing of Sarbanes Oxley in 2002 put the spotlight on tighter internal controls for financial reporting and the new standards passed by the AICPA in 2006 and 2007 increased the controls over information technology (Schroeder & Singleton, 2010). As an organization increases the amount of internal controls it has, it makes it easier for auditors to assess their information systems (Schroeder & Singleton, 2010). A major determinant of information systems auditing is IT Governance, which is defined by the ISACA as "consists of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives" (Marks, 2010). One way IT Governance is controlled is through using COSO's Internal Control-Integrated Framework (Klamm & Watson, 2009). COSO's framework helps assess the internal control environment along with monitoring of the information systems, which helps a firm maintain proper IT Governance (Klamm & Watson, 2009). The use of new technology can help a company be innovative with their IT

Governance; making controls more efficient (Lack of IT, 2005). Without proper IT Governance, which is overseen by the board of directors, then the organization is not likely to have a positive audit of their information systems (Marks, 2010). Each system should also be monitored to ensure that it is compliant with all rules and regulations issues by SOX (Marks, 2010). Once internal controls are in place the organization should be ready for a proper audit of their information systems.

The use of auditors for information systems helps ensure that the organization is mitigating as much risk as possible. This is important because the organization has to issue reliable financial reports under SOX 404 (Nagy, 2010). When auditors are looking at an organization's information systems it is important to look at the entire organization and their employees (Marks, 2010). The auditor should also become familiar with the organization and the type of business they conduct. Once the auditor is knowledgeable with the organization, the auditors should setup a formal audit plan before auditing the information systems. These include assessing the role of IT in financial reports, the potential for errors and fraud and how the information flows (Schroeder & Singleton, 2010). Once the audit is planned out and items are lined up to be assessed, the audit can begin. It is important for the auditors to focus on the items that could potential have material effects on the financial statements (Schroeder & Singleton, 2010). If any major items are found in the audit, the auditor must address the deficiency and the organization must correct the issues in order to gain the confidence of the stakeholders (Schroeder & Singleton, 2010). Once an organization has strong internal controls over their information systems and goes through a proper audit, they can continue to mitigate risk on a day to day basis. The system should continue to be monitored to ensure that it is compliant with all rules and regulations issues by SOX (Marks, 2010).

Although having proper internal controls and audits in place over information systems is crucial, it is also incredibly expensive for organizations of all sizes to implement the proper controls in order to successfully pass an audit. In a survey done by CRA in 2006, the average cost of internal controls and SOX compliance was \$900,000 for small businesses and \$4,300,000 for larger organizations (Noel, 2006). While the controls can be costly, SOX requires them and if done properly the Return on security investment or ROSI can outweigh the cost (Drugescu, 2006). The return will most likely be greater when the company uses the appropriate technology to make the controls more efficient (Drugescu, 2006). By installing proper metrics an organization can continuously monitor the security that is in place for suitable controls and they will be able to report back to the board the effectiveness of the controls (Drugescu, 2006). Furthermore, another survey done by Financial Executives International found that “compliance with Section 404 has resulted in more investor confidence in financial reports [and] financial reports are more reliable” (Noel, 2006). The results of this survey are backed up by a survey of audit professionals that states that the benefits of business process improvement are beginning to outweigh the cost in 2010 (Cain, 2010). This shows that even though auditing of information systems and proper internal controls can be costly, the benefits outweigh the cost.

After the passing of Sarbanes Oxley in 2002, it is imperative for organizations to have proper internal controls over their information systems. These controls need to be audited and any risks that are assessed by the auditors need to be addressed to ensure that the financial reports that are issued do not contain any misleading information. Although the cost to implement these controls can be expensive, the benefits of having stakeholders that trust the information reported outweigh these costs.

References

- Cain, A. (2010) Leading Security Concerns in 2010. *Internal Auditor*, 67(4) 16-7. Retrieved from Business Source Premier database.
- Drugescu, C., & Etges, R. (2006). Maximizing the Return on Investment on Information Security Programs: Program Governance and Metrics. *Information Systems Security*, 15(6), 30-40.
- Johnson, E. (2005, September). Performance vehicles. *Management*, 9, Retrieved from www.managment.co.nz
- Klamm, B., & Watson, M. (2009). SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology. *Journal of Information Systems*, 23(2), 1-23. Retrieved from Business Source Premier database.
- Lack of IT Governance is Putting Business Value at Risk. (2007). Manufacturing business Technology. *Highlands Ranch*, 25(8), 46.
- Marks, N. (2010). The Pulse of IT Governance. *Internal Auditor*, 67(4), 32-37. Retrieved from Business Source Premier database.
- Masli, A., Peters, G., Richardson, V., & Sanchez, J. (2010). Examining the Potential Benefits of Internal Control Monitoring Technology. *Accounting Review*, 85(3), 1001-1034. Retrieved from Business Source Premier database.
- Nagy, A. (2010). Section 404 Compliance and Financial Reporting Quality. *Accounting Horizons*, 24(3), 441-454. doi:10.2308/acch.2010.24.3.441.

Noel, J. SOX and IT Controls- The Story Behind the Woes. *Software*

Mag.com. www.softwaremag.com

Schroeder & Singleton, D. & Singleton, T. (2010). Implementing the IT- Related Aspects of Risk-Based Auditing Standards. *CPA Journal*, 80(7), 66-71. Retrieved from Business Source Premier Database.